UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,214	04/18/2001	Peter T. Dinsmore	NAI1P089/00.175.01	6427

28875 7590 07/24/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/836,214	DINSMORE ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-15,17-21,28-30 and 38-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 10 May 2006 has been noted and made of record.

2. Claims 1-41 have been presented for examination.

3. Claims 10, 16, 22-27, and 31-37 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments filed 10 May 2006 have been fully considered but they are not persuasive.

5. In response to the Applicant's argument that the cited reference does not disclose wherein the updating does not use new secret information, the Examiner disagrees. The Examiner directs the Applicant's attention to MPEP § 2131, in particular the discussion of *ipsissimis verbis*. *Ipsissimis verbis* states that the elements of the invention must be arranged as required by the claim regardless of the identity of terminology. In other words, the fact that Gundavelli does not use the same terminology as the Applicant, yet teaches the elements of the claim language, is not enough to distinguish the instant application over the prior art.

6. Where applicant acts as his or her own lexicographer to specifically define a term of a claim, the written description must clearly define the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The Applicant fails to meet the requirements of defining a term, such as "secret information," as set forth in the MPEP § 2106. In order to define/redefine a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must " set out his uncommon definition in some manner within the patent disclosure' so as to give one

of ordinary skill in the art notice of the change" in meaning. The Examiner has interpreted secret as key, and new secret information as generating a new key. As Gundavelli states in the cited sections that a new group key is generated using the traditional Diffie-Hellman approach, which is to generate a group key using the members already existing keys. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

7. Therefore, Gundavelli discloses updating a secret without using new secret information.

8. In response to the Applicant's argument that the prior art does not disclose that knowledge of the first key and updated first key does not give any knowledge of said second key, the Examiner disagrees. The Applicant claims descriptive material that is the reasoning behind updating the compromised key, it allows for the updating of the group key without compromising any member of the group's key.

9. Therefore, Gundavelli discloses knowledge of the first key and updated first key does not give any knowledge of said second key, thereby making the keys resistant to collusion attacks.

10. See further rejections that follow.

Claim Rejections - 35 USC § 102

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims 1-6, 8-16, 19-21, and 40 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,941,457 to Gundavelli et al., hereinafter Gundavelli.

13. As per claim 1, Gundavelli discloses an environment that includes a plurality of users, wherein each user possess secrets that are shared by respective sets of said plurality of users, a secret updating method, comprising:

(a) updating at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user, wherein said updating does not use new secret information (column 5, lines 47-63, column 11, lines 6-39).

14. Regarding claim 2, Gundavelli teaches wherein said updating comprises updating a plurality of compromised secrets (column 11, lines 6-18, i.e. techniques are applicable in which members are deleted).

15. Regarding claim 3, Gundavelli discloses wherein said updating comprises updating all compromised secrets (column 11, lines 18-25, i.e. remaining members use newly established secret key).

16. Regarding claim 4, Gundavelli discloses wherein said updating comprises updating at least one compromised secret known by one evicted user (column 5, lines 47-63, column 11, lines 6-39).

17. With regards to claims 5, 14, and 15, Gundavelli teaches wherein said updating occurs upon an eviction event, wherein only said second user or the second user and one or more other

users are evicted (column 5, lines 47-63, column 11, lines 6-18, i.e. member departs, members are deleted).

18. Regarding claim 6, Gundavelli teaches wherein said updating comprises updating at least one compromised secret known by a plurality of evicted users (column 11, lines 6-18, i.e. techniques are applicable in which members are deleted).

19. Regarding claim 8, Gundavelli teaches wherein said updating comprises updating a compromised secret using one non-compromised secret (column 5, lines 47-63, column 11, lines 6-39).

20. Regarding claim 9, Gundavelli teaches wherein said updating comprises updating a compromised secret known by a set of users using a non-compromised secret of a subgroup of said set of users (column 5, lines 47-63, column 11, lines 6-39).

21. Regarding claim 11, Gundavelli teaches wherein said compromised secret is shared by said plurality of users (column 5, lines 47-63, column 11, lines 6-39).

22. Regarding claim 12, Gundavelli teaches wherein said secrets enables secure communication (column 11, lines 15-18, i.e. multicast group can communicate over a secure channel).

23. As per claim 13, Gundavelli teaches an environment that includes a plurality of users, wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of sets, said set of users including at least said first user and a second user, a keying method, comprising:

(a) upon eviction of at least said second user, determining an updated first key using information that includes said first key and a second key, wherein said second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction (column 5, lines 47-63, column 11, lines 6-39, i.e. forming new group with no evicted users)

(1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key (column 5, lines 47-63, column 11, lines 6-39).

24. Regarding claim 19, Gundavelli teaches wherein said determining uses only said first key and said second key (column 5, lines 47-63, column 11, lines 6-39).

25. Regarding claims 20 and 21, Gundavelli teaches wherein said subgroup includes only said first user or a plurality of users (column 5, lines 47-63, column 11, lines 6-39).

26. Regarding claim 40, Gundavelli discloses wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user (column 11, lines 6-39).

27. Claims 28-30 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,240,188 to Dondeti et al., hereinafter Dondeti.

28. As per claim 28, Dondeti teaches a keying method in an environment having a plurality of users, each user being capable of storing a set of keys that enable secure communication among sets of said plurality of users, comprising:

(a) distributing first information that enables users to update, after eviction of one or more users, a set of compromised keys that are known to said one or more users without receiving new key information, wherein said update does not include new secret information (column 8, line 43 to column 9, line 19).

29. Regarding claim 29, Dondeti discloses wherein said first information includes information that enables identification of a one-way function (column 3, line 64 to column 4, line 21).

30. Regarding claim 30, Dondeti teaches wherein said first information includes information that enables identification of said evicted one or more users (column 8, line 43 to column 9, line 19).

31. Claims 38 and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,295,361 to Kadansky et al., hereinafter Kadansky.

32. As per claims 38 and 39, Kadansky discloses a secret sharing system, comprising:

a key server that distributes secret information to a plurality of users, wherein each user is sent secrets that are shared by respective sets of said plurality of users, said key server being operative to update at least one compromised secret known by at least one evicted user at least one non-compromised secret that is not known by said at least one evicted user (column 1, line 66 to column 2, line 61).

33. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gundavelli in view of U.S. Patent No. 6,178,244 to Takeda, hereinafter Takeda.

34. With regards to claim 7, Gundavelli does not teach wherein said updating occurs on a periodic basis.

35. Takeda teaches wherein said updating occurs on a periodic basis (column 12, lines 38-43).

36. Both Gundavelli and Takeda both disclose updating keys for group communication.

37. It would have been obvious to one of ordinary skill in the art at the time the invention was made to update the keys on a periodic basis, since Gundavelli states at column 7, lines 25-38, that the communication occurs over the Internet and therefore may be subject to sniffing, or the spying of packets. Therefore, one of ordinary skill would recognize that changing the key periodically would make it more difficult for an eavesdropper to intercept group communications.

38. Claims 17, 18, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gundavelli in view Dondeti.

39. With regards to claims 17 and 41, Gundavelli does not disclose wherein said determining uses a one-way function.

40. Dondeti teaches wherein said determining uses a one-way function (column 3, line 64 to column 4, line 21).

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine the new key using a one-way function, since Dondeti states at column 4, lines 7-21 that such a modification would make it computationally infeasible to compute the key.

42. Concerning claim 18, Gundavelli teaches wherein said updated first key is equal to F(first key, second key) (column 5, lines 47-63, column 11, lines 6-39).

43. Gundavelli does not teach wherein F() is a one-way function.

44. Dondeti teaches wherein F() is a one-way function (column 3, line 64 to column 4, line 21).

45. It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine the new key using a one-way function, since Dondeti states at column 4, lines 7-21 that such a modification would make it computationally infeasible to compute the key.

Conclusion

46. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

47. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Thursday 7-5.

49. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

50. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

CHRISTOPHER REVAK
PRIMARY EXAMINER

7/22/06